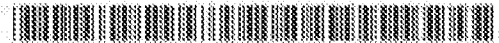


(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001年2月22日 (22.02.2001)

PCT

(10) 国際公開番号
WO 01/13358 A1(51) 国際特許分類: G10K 15/02, G06F
15/00, 17/60, H04L 9/08, 9/32, G06K 19/00, H04H 1/00,
H04M 3/42, 3/493, 11/08, G01L 19/00

(21) 国際出願番号: PCT/JP00/05339

(22) 国際出願日: 2000年8月9日 (09.08.2000)

(25) 国際出願の言語: 日本語

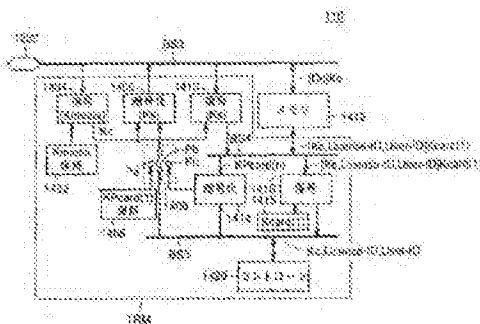
(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/226406 1999年8月10日 (10.08.1999) JP
特願平11/349336 1999年12月8日 (08.12.1999) JP(71) 出願人 (米国を除く全ての指定国について): 富士通
株式会社 (FUJITSU LIMITED) [JP/JP] 〒211-8588 神
奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa(JP) 日本コロムビア株式会社 (NIPPON COLUMBIA
CO., LTD.) [JP/JP] 〒107-8011 東京都港区赤坂四丁目
14番14号 Tokyo (JP). 株式会社日立製作所 (HITACHI
LTD.) [JP/JP] 〒101-8010 東京都千代田区神田駿河台
四丁目6番地 Tokyo (JP). 三洋電機株式会社 (SANYO
ELECTRIC CO., LTD.) [JP/JP] 〒570-8677 大阪府守
口市京阪本通2丁目5番5号 Osaka (JP).(72) 発明者: および
(75) 発明者/出願人 (米国についてのみ): 畑中正行
(HATANAKA, Masayuki) [JP/JP] 蒲田 順 (KA-
MADA, Jun) [JP/JP] 畠山卓久 (HATAKEYAMA,
Takahisa) [JP/JP] 長谷部高行 (HASEBE, Takayuki)
[JP/JP] 小谷誠剛 (KOTANI, Seigou) [JP/JP] 古田茂
樹 (FURUTA, Shigeki) [JP/JP] 〒211-8588 神奈川県
川崎市中原区上小田中4丁目1番1号 富士通株式
社内 Kanagawa (JP). 穴澤健明 (ANAZAWA, Takeaki)
[JP/JP] 〒107-8011 東京都港区赤坂四丁目14番14
号 日本コロムビア株式会社内 Tokyo (JP). 利根川

/続業者/

(54) Title: MEMORY CARD

(54) 発明の名称: メモリカード





忠明 (TONEGAWA, Tadaaki) [JP/JP]: 〒157-8588 東京都小平市上水本町五丁目20番1号 株式会社日立製作所 半導体グループ内 Tokyo (JP). 日置敏昭 (HIKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 堀 吉宏 (HORI, Yoshitiro) [JP/JP]: 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP).

(74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.): 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AI, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, GR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MY, NZ, PL,

PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PC7ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

メモ리카ード

5 技術分野

本発明は、携帯電話等の端末に対して情報を配送するための情報配信システムにおいて、コピーされた情報に対する著作権保護を可能とするメモ리카ードに関するものである。

10 背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽情報や映像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行な

う個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

しかも、CDからMDへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、1つのMDからさらに他のMDに音楽データをデジタル情報としてコピーすることは、著作権者保護のために機器の構成上できないようになっている。

すなわち、現状においては、デジタル記録媒体であるCDからMDへのコピーは、自由に行なうことができるものの、記録可能なMDからMDへのコピーを行なうことはできない。

そのような事情からも、音楽情報や画像情報をデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権限のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権限を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

発明の開示

本発明の目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムにおけるメモリカードを提供することである。

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムにおけるメモリカードを提供することである。

係る目的を達成するために本願発明に係るメモリカードは、暗号化コンテンツデータを受けて記録するためのメモリカードであって、第1の鍵保持部と、第1の復号処理部と、第2の鍵保持部と、第1の暗号化処理部と、第2の復号処理部と、第1の記憶部と、第3の鍵保持部と、第3の復号処理部とを備える。

第1の鍵保持部は、メモ리카ードに対応して予め定められた第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する。

第1の復号処理部は、暗号化コンテンツデータの通信ごとに更新されて配信され、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理する。

第2の鍵保持部は、メモ리카ードごとに異なる第2の公開暗号化鍵を保持する。第1の暗号化処理部は、第2の公開暗号化鍵を、第1の共通鍵に基づいて暗号化し、出力する。

第2の復号処理部は、第2の公開暗号化鍵で暗号化され、さらに第1の共通鍵で暗号化されたコンテンツキーを受け、第1の共通鍵に基づいて復号化する。第1の記憶部は、第2の復号処理部の出力を受けて、格納する。第3の鍵保持部は、第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する。第3の復号処理部は、第1の記憶部に格納されたデータに基づいて、第2の秘密復号鍵によりコンテンツキーを復号する。

本発明の他の局面に従うと、暗号化データと暗号化データを復号するための復号情報データを受けて記録するためのメモ리카ードであって、第1の記憶部と、第1の鍵保持部と、第2の鍵保持部と、第1の復号処理部と、第3の鍵保持部と、セッションキー発生部と、第1の暗号化処理部と、第2の復号処理部と、第2の記憶部と、第4の鍵保持部と、第3の復号処理部とを備える。

第1の記憶部は、暗号化データを格納する。第1の鍵保持部は、メモ리카ードに対応して予め定められた第1の公開暗号化鍵と自身の認証データとを公開認証鍵により復号できるように暗号化して保持し、外部に対して出力可能である。

第2の鍵保持部は、第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する。第1の復号処理部は、復号情報データの通信ごとに更新されて送信され、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理する。

第3の鍵保持部は、メモ리카ードごとに異なる第2の公開暗号化鍵を保持する。セッションキー発生部は、復号情報データの通信ごとに更新される第2の共通鍵を生成する。第1の暗号化処理部は、第2の公開暗号化鍵と第2の共通鍵を、

第1の共通鍵に基づいて暗号化し、出力する。第2の復号処理部は、外部にて第2の公開暗号鍵によって暗号化され、さらに第2の共通鍵によって暗号化された復号情報データを第2の共通鍵に基づいて復号する。

5 第2の記憶部は、第2の復号処理部の出力である第2の公開暗号鍵によって暗号化された復号情報データを格納する。第4の鍵保持部は、第2の公開暗号化鍵によって暗号化されたデータを復号するための第2の秘密復号鍵を保持する。第3の復号処理部は、第2の記憶部に格納されたデータを第2の秘密復号鍵に基づいて復号し、復号情報データを抽出する。

10 この発明のさらに他の局面に従うと、暗号化データと暗号化データを復号するための復号情報データを受けて記録するためのメモリカードであって、第1の記憶部と、第1の鍵保持部と、第2の鍵保持部と、第1の復号処理部と、第3の鍵保持部と、セッションキー発生部と、第1の暗号化処理部と、第2の復号処理部と、第4の鍵保持部と、第3の復号処理部と、第2の記憶部とを備える。

15 第1の記憶部は、暗号化データを格納する。第1の鍵保持部は、メモリカードに対応して予め定められた第1の公開暗号化鍵と自身の認証データとを公開認証鍵により復号できるように暗号化して保持し、外部に対して出力可能である。

20 第2の鍵保持部は、第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する。第1の復号処理部は、復号情報データの通信ごとに更新されて送信され、第1の公開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理する。第3の鍵保持部は、メモリカードごとに異なる第2の公開暗号化鍵を保持する。

セッションキー発生部は、復号情報データの通信ごとに更新される第2の共通鍵を生成する。第1の暗号化処理部は、第2の公開暗号化鍵と第2の共通鍵を、第1の共通鍵に基づいて暗号化し、出力する。

25 第2の復号処理部は、外部にて第2の公開暗号鍵によって暗号化され、さらに第2の共通鍵によって暗号化された復号情報データを第2の共通鍵に基づいて復号する。

第4の鍵保持部は、第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する。

第3の復号処理部は、外部にて第2の公開暗号化鍵によって暗号化された復号情報データを受けて、第2の秘密復号鍵により復号情報データを復号する。第2の記憶部は、復号情報データを格納する。

したがって、本発明によれば、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となり、かつ、1度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

図面の簡単な説明

図1は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

図2は、図1に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

図3は、図1に示したコンテンツサーバ10の構成を示す概略ブロック図である。

図4は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

図5は、図4に示したメモリカード110の構成を説明するための概略ブロック図である。

図6は、図1および図3～図5で説明したデータ配信システムにおける配信モードを説明するためのフローチャートである。

図7は、実施例1の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図8は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートである。

図9は、暗号化されたコンテンツデータの複製を行なうモードを説明するためのフローチャートである。

図10は、本発明の実施例2のメモリカード130の構成を説明するための概略ブロック図である。

図11は、メモリカード130の移動モードを説明するためのフローチャートである。

5 図12は、本発明の実施例3のメモリカード140の構成を説明するための概略ブロック図である。

図13は、図12で説明したメモリカード140を用いた配信モードを説明するためのフローチャートである。

10 図14は、実施例3の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図15は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

図16は、暗号化されたコンテンツデータの複製を行なうモードを説明するためのフローチャートである。

15 図17は、実施例3の変形例の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図18は、本発明の実施例4のメモリカード150の構成を説明するための概略ブロック図である。

20 図19は、メモリカード150の移動モードを説明するためのフローチャートであり、実施例2の図11と対比される図である。

図20は、本発明の実施例5のメモリカード160の構成を説明するための概略ブロック図である。

図21は、図20で説明したメモリカード160を用いた配信モードを説明するためのフローチャートである。

25 図22は、実施例5の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

図23は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートである。

図24は、本発明の実施例6のメモリカード170の構成を説明するための概

略ブロック図である。

図25は、メモ리카ード170の移動モードを説明するためのフローチャートである。

5 図26は、実施例7の携帯電話機101の構成を説明するための概略ブロック図である。

図27は、実施例7のメモ리카ード180に対応したコンテンツサーバ11の構成を示す概略ブロック図である。

図28は、本発明の実施例7のメモ리카ード180の構成を説明するための概略ブロック図である。

10 図29は、本発明の実施例7のメモ리카ード180を用いた配信モードを説明するためのフローチャートである。。

図30は、実施例7の暗号化コンテンツデータを復号し音楽データとして出力する再生モードを説明するフローチャートである。

15 図31は、2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートである。

図32は、実施例8における携帯電話機105の構成を説明するための概略ブロック図である。

図33は、実施例8のメモ리카ード190に対応したコンテンツサーバ12の構成を示す概略ブロック図である。

20 図34は、本発明の実施例8のメモ리카ード190の構成を説明するための概略ブロック図である。

図35は、実施例8のメモ리카ード190の記録領域の配置を示す概略図である。

25 図36は、図35で説明したメモ리카ード190を用いた配信モードを説明するためのフローチャートである。

図37は、メモ리카ード190に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生モードを説明するフローチャートである。

図38は、実施例8の2つのメモ리카ード間において、移動を行なう処理を説明するためのフローチャートである。

図39は、実施例9のメモ리카ード200の構成を示す概略ブロック図である。

図40は、実施例9のメモ리카ード200の記録領域の配置を示す概略ブロック図である。

5 図41は、図38で説明したメモ리카ード200を用いた配信モードを説明するためのフローチャートである。

図42は、メモ리카ード200に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生モードを説明するフローチャートである。

図43は、実施例9の2つのメモ리카ード間において、移動を行なうモードを説明するためのフローチャートである。

10

発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

〔実施例1〕

15 図1は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

なお、以下では携帯電話網を介して、音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物データ、たとえば画像データ等の著作物データを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

20

図1を参照して、著作権の存在する音楽情報を管理するコンテンツサーバ10は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア20である携帯電話会社に、このような暗号化データを与える。

25

配信キャリア20は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）をコンテンツサーバ10に中継する。コンテンツサーバ10は配線リクエストに応じて、要求されたコンテンツデータをさらに暗号化したうえで、配信キャリア20の携帯電話網を介して、各ユーザの携帯電話機に対して配信する。

図1においては、たとえば携帯電話ユーザ1の携帯電話機100には、携帯電話100により受信された暗号化されたコンテンツデータを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機100中の音楽再生部（図示せず）に与えるための着脱可能なメモリカード110に格納する構成となっている。

さらに、たとえばユーザ1は、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを再生した音楽を聴取することが可能である。

以下では、このようなコンテンツサーバ10と配信キャリア20とを併せて、音楽サーバ30と総称することにする。

また、このような音楽サーバ30から、各携帯電話端末にコンテンツデータを伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、正規のメモリカードであるメモリカード110を購入していないユーザは、音楽サーバ30からの配信データを受取って再生することが困難な構成となる。

しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このようなコンテンツデータの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

このとき、たとえばメモリカード112を有するユーザ2が、自己の携帯電話機102により、音楽サーバ30から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等をユーザ2が直接音楽サーバ30から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ1から、そのコンテンツデータをコピーできるこ

とを可能としておけば、ユーザにとっての利便性が向上する。

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

図1に示した例では、ユーザ1が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、ユーザ2に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合、ユーザ1は、再生のために必要な情報（再生情報）ごとユーザ2にコピーさせるため、情報の移動を行なった後には、ユーザ1においてはコンテンツデータの再生を行なうことは不可能とする必要がある。ここで、コンテンツデータとは所定の暗号化方式に従って暗号化された暗号化コンテンツデータとして配信され、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたがって暗号化されたコンテンツデータを復号可能なライセンスキーと、ライセンスIDデータ License-ID、ユーザIDデータ User-ID等のライセンス情報とを意味する。

これに対して、コンテンツデータのみを暗号化されたままの状態、ユーザ2にコピーさせることを音楽情報の「複製」と呼ぶこととする。

この場合、ユーザ2の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされない、ユーザ2は、暗号化されたコンテンツデータを得ただけでは、音楽を再生させることができない。したがって、ユーザ2が、このような音楽の再生を望む場合は、改めて音楽サーバ30からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよい、ユーザ2が直接音楽サーバ30からすべての配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

たとえば、携帯電話機100および102が、PHS（Personal Handy Phone）（登録商標）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ1からユーザ2への一括した情報の移転（移動）や、暗号化したコンテンツデータのための転送（複製）を行なうことが可能である。

図1に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号化キー（鍵）を配送するための方式であり、さらに第2には、配信データを暗号化する方式そのものであり、さらに、第3には、このようにして配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

図2は、図1に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図1に示した構成において、メモ리카ード100内のデータ処理を管理するための鍵としては、メモ리카ードという媒体の種類に固有で、すべてのメモ리카ードに対して共通な秘密復号鍵 K_{media} と、メモ리카ードごとに異なる公開暗号化鍵 $K_{Pcard}(n)$ と、公開暗号化鍵 $K_{Pcard}(n)$ により暗号化されたデータを復号するための秘密復号鍵 $K_{card}(n)$ とがある。

ここで、秘密復号鍵 $K_{card}(n)$ や秘密復号鍵 $K_{Pcard}(n)$ の表記中の自然数 n は、各ユーザ（メモ리카ード）を区別するための番号を表わす。

すなわち、公開暗号化鍵 $K_{Pcard}(n)$ で暗号化されたデータは、各メモ리카ードごとに存在する秘密復号鍵 $K_{card}(n)$ で復号可能である。したがって、メモ리카ードにおける配信データの授受にあたっては、基本的には、後に説明するように3つの鍵 K_{media} 、 $K_{card}(n)$ 、 $K_{Pcard}(n)$ が用いられることになる。

さらに、メモ리카ード外とメモ리카ード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有、すなわち、メモ리카ードすべてに共通な公開暗号化鍵 K_{Pmedia} と、公開暗号化鍵 K_{Pmedia} により暗号化されたデータを復号するための秘密復号鍵 K_{media} と、各通信ごと、たとえば、音楽サーバ30へのユーザのアクセスごとに生成される共通鍵 K_s が用いられる。

ここで、共通鍵 K_s は、上述のとおり、ユーザが音楽サーバ30に対して1回のアクセスを行なうごとに発生する構成として、1回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、た

例えば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵 K_s を「セッションキー」とも呼ぶことにする。

- 5 したがって、共通鍵 K_s は各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

- また、配信されるべきデータについては、まず、暗号化されたコンテンツデータを復号する鍵である K_c （以下、ライセンスキーと呼ぶ）があり、このライセンス鍵 K_c により暗号化されたコンテンツデータが復号化されるものとする。さらに、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンスIDデータ $License-ID$ と、受信者を識別するためのユーザIDデータ $User-ID$ 等が存在する。ここで、ユーザIDデータ $User-ID$ としては、たとえばユーザの電話番号等を用いることが可能である。

- 15 このような構成とすることで、ライセンスIDデータ $License-ID$ に含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザIDデータ $User-ID$ を用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

- 20 配信データにおけるコンテンツデータ D_c は、上述のとおり、たとえば音楽データであり、このコンテンツデータをライセンスキー K_c で復号化可能なデータを、暗号化コンテンツデータ $[D_c] K_c$ と呼ぶ。

ここで、 $[Y] X$ という表記は、データ Y を、キー X により復号可能な暗号に変換した情報であることを示している。

- 25 図3は、図1に示したコンテンツサーバ10の構成を示す概略ブロック図である。コンテンツサーバ10は、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンスIDデータ $License-ID$ 等の配信情報を保持するための配信情報データベース304と、各ユーザごとにコンテンツデータへのアクセス回数等に従った課金情報を保持するための課金データベ

ース302と、配信情報データベース304および課金データベース302からのデータをデータバスBS1を介して受取り、所定の暗号化処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

5 データ処理部310は、データバスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部312と、配信制御部312に制御されて、セッションキー K_s を発生するためのセッションキー発生部314と、セッションキー発生部314より生成されたセッションキー K_s を、公開暗号化鍵 $KPmedia$ により暗号化して、データバスBS1に与えるための暗号化処理部316と、各ユーザの携帯電話機においてセッションキー K_s により暗号化されたうえで送信されたデータを通信装置350およびデータバスBS1を介して受けて、復号処理を行なう復号処理部318と、復号処理部318により抽出された公開暗号化鍵 $KPcard(n)$ を用いて、ライセンスキーやライセンスIDデータ $LICENSE-ID$ 等のデータを配信制御部312に制御されて暗号化するための暗号化処理部320と、暗号化処理部320の出力を、さらにセッションキー K_s により暗号化して、データバスBS1を介して通信装置350に与える暗号化処理部322とを含む。

10
15

図4は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

20 携帯電話機100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのデータバスBS2と、データバスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106と、外部からの指示を携帯電話機100に与えるためのタッチキー部1108と、コントローラ1106等から出力される情報をユーザに視覚情報として与えるためのディスプレイ1110と、通常の通話モードにおいて、データバスBS2を介して与えられる受信データに基づいて音声再生するための音声再生部1112とを備える。

25

携帯電話機100は、さらに、コンテンツサーバ10からのコンテンツデータを復号化処理するための着脱可能なメモリカード110と、メモリカード110とデータバスBS2との間のデータの授受を制御するためのメモリインタフェース1200と、メモリカード110と携帯電話機の他の部分とのデータ授受にあたり、データバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKsを乱数等により発生するセッションキー発生部1502と、セッションキー発生部1502により生成されたセッションキーを公開暗号化鍵Kpmediaで暗号化して、データバスBS2に与えるための暗号化処理部1504と、セッションキー発生部1502において生成されたセッションキーKsに基づいて、データバスBS2上のデータをセッションキーKsにより復号して出力する復号処理部1506と、復号処理部1506の出力を受けて、音楽信号を再生するための音楽再生部1508と、音楽再生部1508の出力と音声再生部1112の出力とを受けて、動作モードに応じて選択的に出力するための混合部1510と、混合部1510の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部1512と、デジタルアナログ変換部1512の出力を受けて、ヘッドホン120と接続するための接続端子1514とを含む。

なお、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

図5は、図4に示したメモリカード110の構成を説明するための概略ブロック図である。

メモリカード110は、メモリインタフェース1200との間で信号を端子1202を介して授受するデータバスBS3と、秘密復号鍵Kmediaを保持するためのKmedia保持部1402と、データバスBS3にメモリインタフェース1200から与えられるデータから、秘密復号鍵Kmediaにより復号処理をすることにより、セッションキーKsを抽出する復号処理部1404と、公開暗号化キーKpcard(1)を保持するためのKpcard(1)保持部1405と、復号処理部1404により抽出されたセッションキーKsに基づいて、

切換えスイッチ1408からの出力を暗号化してデータベースBS3に与えるための暗号化処理部1406と、データベースBS3上のデータを復号処理部1404により抽出されたセッションキーKsにより復号処理してデータベースBS4に与えるための復号処理部1410と、データベースBS4からメモリカードごとに異なる公開暗号化鍵K P c a r d (n)で暗号化されているライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータ U s e r - I D等のデータを格納し、データベースBS3からライセンスキーKcにより暗号化されている暗号化コンテンツデータ[Dc] Kcを受けて格納するためのメモリ1412とを備える。

- 10 切換えスイッチ1408は、接点Pa、Pb、Pcを有し、接点PaにはK P c a r d (1)保持部1405からの暗号化キーK P c a r d (1)が、接点PbにはデータベースBS5が、接点Pcには暗号化処理部1414の出力が与えられる。切換えスイッチ1408は、それぞれ、接点Pa、Pb、Pcに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」の
15 いずれであるかに応じて、選択的に暗号化処理部1406に与える。

- メモリカード110は、さらに、秘密復号キーK c a r d (1)の値を保持するためのK c a r d (1)保持部1415と、公開暗号化鍵K P c a r d (1)により暗号化されており、かつ、メモリ1412から読出されたライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータ U s e r - I D等（[Kc, L i c e n s e - I D, U s e r - I D] K c a r d (1)）を、復号処理してデータベースBS5に与える復号処理部1416と、データの移動処理等において、相手先のメモリカードの公開暗号化鍵K P c a r d (n)を復号処理部1410から受けて、この相手方の公開暗号化鍵K P c a r d (n)に基づいて、データベースBS5上に出力されているライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータ U s e r - I D等を暗号
20 化したうえで、切換えスイッチ1408に出力するための暗号化処理部1414と、データベースBS5との間でライセンスIDデータL i c e n s e - I D、ユーザIDデータ U s e r - I D等を受けて、メモリカード110の動作を制御するためのコントローラ1420とを備える。
25

なお、図5において実線で囲んだ領域は、メモ리카ード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読み出しを不能化するためのモジュールTRMに組込まれているものとする。

5 このようなモジュールは、一般にはタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

もちろん、メモリ1412も含めて、モジュールTRM内に組み込まれる構成としてもよい。しかしながら、図5に示したような構成とすることで、メモリ1412中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ1412中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ1412を設ける必要がないので、製造コストが低減されるという利点がある。

図6は、図1および図3～図5で説明したデータ配信システムにおける配信モードを説明するためのフローチャートである。

15 図6においては、ユーザ1が、メモ리카ード110を用いることで、コンテンツサーバ10からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機100から、ユーザのキーボタンの操作等によって、コンテンツサーバ10に対して配信リクエストがなされる (ステップS100)。

20 コンテンツサーバ10においては、この配信リクエストに応じて、セッションキー発生部314が、セッションキー K_s を生成する (ステップS103)。

続いて、サーバ内の暗号化処理部316が、公開暗号化キー K_{Pmedia} により、セッションキー K_s を暗号化処理して、データバスBS1に与える (ステップS104)。

25 通信装置350は、暗号化処理部316からの暗号化セッションキー $[K_s]$ K_{media} を、通信網を通じて、携帯電話機100のメモ리카ード110に対して送信する (ステップS106)。

メモ리카ード110においては、メモリインタフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、 K_{media}

a 保持部1402から与えられる秘密復号キー K_{media} により復号処理することにより、セッションキー K_s を復号し抽出する（ステップS108）。

5 続いて、配信モードにおいては、切換えスイッチ1408は、接点 P_a が閉じる状態が選択されているので、暗号化処理部1406は、接点 P_a を介して $K_{Pcard(1)}$ 保持部1405から与えられる公開暗号化鍵 $K_{Pcard(1)}$ （ユーザ1のメモリカードにおける公開暗号化鍵）を、セッションキー K_s により暗号化して、データバスBS3に与える（ステップS110）。

10 携帯電話機100は、暗号化処理部1406により暗号化されたデータ $[K_{Pcard(1)}] K_s$ をコンテンツサーバ10に対して出力する（ステップS112）。

コンテンツサーバ10では、通信装置350により受信され、データバスBS1に与えられたデータ $[K_{Pcard(1)}] K_s$ を復号処理部318が、セッションキー K_s により復号化処理して、公開暗号化キー $K_{Pcard(1)}$ を復号抽出する（ステップS114）。

15 続いて、配信制御部312は、ライセンスキー K_c を配信情報データベース304より取得し（ステップS116）、かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータ $License-ID$ およびユーザIDデータ $User-ID$ 等のライセンス情報を生成する（ステップS118）。

20 暗号化処理部320は、配信制御部312からのライセンスキー K_c 、ライセンスIDデータ $License-ID$ およびユーザIDデータ $User-ID$ 等のデータを受取って、復号処理部318より与えられた公開暗号化キー $K_{Pcard(1)}$ により暗号化処理する（ステップS120）。

25 暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキー K_s により暗号化して、データバスBS1に与える（ステップS122）。

通信装置350は、暗号化処理部322により暗号化されたデータ $[[K_c, License-ID, User-ID] K_{card(1)}] K_s$ をカード110に対して送信する。

メモ리카ード110においては、復号処理部1410がセッションキー K_s により、復号処理を行ない、データ $[K_c, License-ID, User-ID]$ $K_{card}(1)$ を抽出し(ステップS126)、メモリ1412に格納する(ステップS128)。

- 5 一方、コンテンツサーバ10は、暗号化コンテンツデータ $[D_c]$ K_c を配信情報データベース304より取得して、通信装置350を介して、メモ리카ード110に送信する(ステップS130)。

メモ리카ード110においては、受信したデータ $[D_c]$ K_c をそのままメモリ1412に格納する(ステップS132)。

- 10 以上のような動作により、メモ리카ード110が格納するコンテンツデータは再生可能な状態となるので、以下では、メモ리카ードが格納するコンテンツデータが再生可能な状態となっていることを、「メモ리카ード110は、状態SAにある」と呼ぶことにする。

- 15 図7は、携帯電話機100内において、メモ리카ード110に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図7を参照して、携帯電話機100のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモ리카ード110に対して出力される(ステップS200)。

- 20 メモ리카ード110では、メモリ1420から、暗号化されているライセンスキー K_c 、ライセンスIDデータ $License-ID$ 、ユーザIDデータ $User-ID$ 等を読み出し(ステップS203)、秘密復号キー $K_{card}(1)$ によって、ライセンスキー K_c 、ライセンスIDデータ $License-ID$ やユーザIDデータ $User-ID$ を復号処理する(ステップS204)。

- 25 コントローラ1420は、復号化されたライセンスIDデータ $License-ID$ 等に含まれる情報に基づいて、復号可能なデータに対するリクエストであるかを判断し(ステップS206)、復号可能と判断した場合は、携帯電話機のコントローラ1106に対して、再生許可通知を送信する(ステップS208)。

携帯電話機100においては、セッションキー発生回路1502がセッション

キー K_s を生成し（ステップS210）、暗号化処理部1504が、公開暗号化キー K_{Pmedia} によりセッションキー K_s を暗号化して（ステップS212）、データベースBS2に暗号化セッションキー $[K_s] K_{media}$ が出力される（ステップS214）。

- 5 メモリカード110は、データベースBS2を介して、携帯電話機100により生成された暗号化セッションキーを受け取り、秘密復号キー K_{media} により復号し抽出する（ステップS216）。

- 続いて、メモリカード110は、抽出したセッションキー K_s により、ライセンスキー K_c を暗号化し（ステップS219）、暗号化ライセンスキー $[K_c] K_s$ をデータベースBS2に与える（ステップS220）。
- 10

 携帯電話機100の復号処理部1506は、セッションキー K_s により復号化処理を行なうことにより、ライセンスキー K_c を取得する（ステップS222）。

 続いて、メモリカード110は、暗号化コンテンツデータ $[D_c] K_c$ をメモリ1412から読出し、データベースBS2に与える（ステップS224）。

- 15 携帯電話機100の音楽再生部1508は、暗号化コンテンツデータ $[D_c] K_c$ を、抽出されたライセンスキー K_c により復号処理し（ステップS226）、コンテンツデータを再生して混合部1510に与える（ステップS228）。

- 一方、ステップS206において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード110は、携帯電話機100に対して、再生不許可通知を送信する（ステップS230）。
- 20

 ステップS230の状態では、コンテンツデータの再生を行なうことができないので、このような状態を以下では「メモリカード110は、状態SBにある」と表現することにする。

- 図8は、2つのメモリカード間において、コンテンツデータおよび再生情報の移動を行なう処理を説明するためのフローチャートである。
- 25

 まず、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。

 携帯電話機100は、まず、自身の側のメモリカード110と、受信側の携帯電話機102に挿入されたメモリカード112に対して、移動リクエストを出力

する（ステップS300）。

さらに、携帯電話機100においては、セッションキー発生回路1502は、セッションキー K_s を生成し（ステップS303）、公開暗号化キー KP_{media} を用いて、暗号化処理部1504がセッションキー K_s を暗号化し（ステップS304）、その暗号化セッションキー $[K_s] K_{media}$ をデータバスBS2を介して、メモリカード110に伝達するとともに、携帯電話機102に装着されたメモリカード112に対して、たとえば、トランシーバモードではアンテナ1102を介して、上記暗号化セッションキー $[K_s] K_{media}$ を伝達する（ステップS306）。

メモリカード110においては、秘密復号キー K_{media} によりセッションキー K_s を復号抽出する（ステップS318）。

同様にして、カード112においても、秘密復号キー K_{media} により、セッションキー K_s を復号抽出し（ステップS320）、さらに、セッションキー K_s によりメモリカード112の公開暗号化キー $KP_{card}(2)$ を暗号化して（ステップS322）、メモリカード110に対して、暗号化されたデータ $[KP_{card}(2)] K_s$ を送信する（ステップS324）。

メモリカード110においては、メモリカード112から送信された暗号化データをセッションキー K_s により復号化して、メモリカード112の公開暗号化キー $KP_{card}(2)$ を復号抽出する（ステップS326）。

続いて、メモリカード110においては、メモリ1412からメモリカード110の公開暗号化キー $K_{card}(1)$ により暗号化されているライセンスキー K_c 、ライセンスIDデータ $License-ID$ およびユーザIDデータ $User-ID$ が読出される（ステップS328）。

続いて、復号処理部1416が、秘密復号キー $K_{card}(1)$ により、ライセンスキー K_c 、ライセンスIDデータ $License-ID$ 、ユーザIDデータ $User-ID$ とを復号処理する（ステップS330）。

さらに、暗号化処理部1414は、復号処理部1410において抽出されたカード112における公開暗号化キー $KP_{card}(2)$ により、ライセンスキー K_c 、ライセンスIDデータ $License-ID$ 、ユーザIDデータ $User-$

IDとを暗号化する（ステップS332）。

暗号化処理部1414により暗号化されたデータは、切換えスイッチ1408（接点Pcが閉じている）を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc, License-ID, User-ID] Kcard(2)をセッションキーKsにより暗号化する（ステップS334）。

続いて、メモ리카ード110は、携帯電話機100を介して、メモ리카ード112に対して、暗号化されたデータ[[Kc, License-ID, User-ID] Kcard(2)] Ksを送信する（ステップS336）。

メモ리카ード112においては、メモ리카ード110から送信されたデータを復号処理部1410により、セッションキーKsに基づいて復号化処理して（ステップS338）、メモリ1412に格納する（ステップS340）。

一方、メモ리카ード110は、さらに、メモリ1412内のデータのうち、ライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-IDに対応したデータを消去する（ステップS342）。

続いて、メモ리카ード110は、暗号化コンテンツデータ[Dc] Kcをメモリから読出し、メモ리카ード112に対して送信する（ステップS344）。

メモ리카ード112は、受信した暗号化コンテンツデータをそのままメモリ1412に格納する（ステップS346）。

以上のような処理を行なうと、ステップS342において、ライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等がメモ리카ード110からは消去されているので、メモ리카ード110は「状態SB」となる。

一方、メモ리카ード112においては、暗号化コンテンツデータ以外にも、ライセンスキー、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等のすべてのデータが移動されているので、メモ리카ード112は「状態SA」となっている。

図9は、図1に示した情報配信システムにおいて、携帯電話機100から携帯電話機102へ、暗号化コンテンツデータの複製を行なう処理を説明するための

フローチャートである。

図9を参照して、携帯電話機100が、メモリカード110およびメモリカード112に対して複製リクエストを出力する（ステップS400）。

5 続いて、メモリカード110は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読出し、メモリカード112に対して出力する（ステップS402）。

メモリカード112においては、メモリカード110から送信された暗号化されたコンテンツデータを、そのままメモリ1412に記録する（ステップS404）。

10 以上のような動作を行なうと、メモリカード110には、暗号化コンテンツデータ、ライセンスキーKc、ユーザIDデータUser-ID、ライセンスIDデータLicense-ID等のすべてのデータが残されているため、メモリカード110は再生可能な状態、すなわち、「状態SA」にある。

一方、メモリカード112は、暗号化コンテンツデータのみを有しているため、
15 そのままでは再生処理を行なうことができない。したがって、この時点ではメモリカード112は、「状態SB」にある。

メモリカード112が状態SAとなるためには、改めてコンテンツサーバ10から、ライセンスキーKc、ライセンスIDデータLicense-IDやユーザIDデータUser-ID等の再生情報を取得する必要がある。

20 以上のような構成とすることで、メモリカードを有する正規のユーザのみがコンテンツデータ（音楽データ）を受信してメモリ中に格納することが可能となり、かつ、1度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより
25 著作権が不当な不利益を被るのを防止することが可能となる。

なお、以上の説明では、コンテンツサーバ10からの暗号化データを復号するための回路は、携帯電話機に着脱可能なメモリカード内に組み込まれる構成としたが、たとえば、携帯電話機内部に作り込まれる構成としてもよい。より一般には、情報サーバにアクセスする端末機器に着脱可能なメモリカード内に組み込ま

れる構成であってもよいし、当該端末機器にあらかじめ組み込まれる構成であってもよい。

[実施例2]

図10は、本発明の実施例2のメモリカード130の構成を説明するための概略ブロック図であり、実施例1の図5と対比される図である。

実施例1のメモリカード110の構成と異なる点は、1つには、メモリカード130内にセッションキー K_s を生成するためのセッションキー発生回路1432が設けられ、かつ、メモリカードという媒体に対応する公開暗号化キー K_{Pmedia} の値を保持する K_{Pmedia} 保持部1440が設けられていることである。メモリカード130は、これに応じて、セッションキー発生回路1432で生成されたセッションキー K_s を、公開暗号化キー K_{Pmedia} により暗号化してデータバスBS3に与えるための暗号化処理部1430と、セッションキー発生回路1432からの出力と復号処理部1404との出力を受けて、選択的に暗号化処理部1406と復号処理部1410に与えるための切換えスイッチ1434を備える構成となっている。

切換えスイッチ1434は、接点Pd、Pe、Pfを有し、接点Pd、Peには、復号処理部1404の出力が、接点Pfにはセッションキー発生回路1432の出力が与えられる。切換えスイッチ1434は、それぞれ、接点Pd、Pe、Pfに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部1406と復号処理部1410に与える。

その他の構成は、図5に示した実施例1のメモリカード110の構成と同様であるの同一部分には同一符号を付して、その説明は繰り返さない。

メモリカード130の動作が、メモリカード110の動作と異なるのは、「移動」処理を行う場合である。

図11は、メモリカード130の移動処理を説明するためのフローチャートであり、実施例1の図8と対比される図である。

図11を参照して、まず、図11においても、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。また、携帯電話機102にも、

メモ리카ード130と同様の構成を有するメモ리카ード132が装着されているものとする。

携帯電話機100は、まず、自身の側のメモ리카ード130と、受信側の携帯電話機102に挿入されたメモ리카ード132に対して、移動リクエストを出力する（ステップS300）。

さらに、携帯電話機100においては、メモ리카ード130内のセッションキー発生回路1432は、セッションキー K_s を生成し（ステップS312）、公開暗号化キー K_{Pmedia} を用いて、暗号化処理部1430がセッションキー K_s を暗号化して（ステップS314）、たとえば、トランシーバモードではアンテナ1102を介して、暗号化されたセッションキー K_s をカード132に伝達する（ステップS316）。

メモ리카ード132においては、復号処理部1404が、秘密復号キー K_{media} により、セッションキー K_s を復号抽出し（ステップS320）、さらに、セッションキー K_s によりメモ리카ード132の公開暗号化キー K_{Pcard} （2）を暗号化して（ステップS322）、メモ리카ード110に対して、暗号化されたデータ $[K_{Pcard}(2)]K_s$ を送信する（ステップS324）。

メモ리카ード110においては、メモ리카ード112から送信された暗号化データをセッションキー K_s により復号化して、メモ리카ード112の公開暗号化キー $K_{Pcard}(2)$ を復号抽出する（ステップS326）。

以下の処理は、基本的に、図8で説明した実施例1の移動処理と同様であるのでその説明は繰り返さない。

以上のような処理を行なうと、ステップS342において、ライセンスキー K_c 、ライセンスIDデータ $License-ID$ およびユーザIDデータ $User-ID$ 等がカード130からは消去されているので、メモ리카ード130は「状態SB」となる。

一方、メモ리카ード132においては、暗号化コンテンツデータ以外にも、ライセンスキー K_c 、ライセンスIDデータ $License-ID$ 、ユーザIDデータ $User-ID$ 等の再生情報が移動されているので、メモ리카ード132は「状態SA」となっている。

以上のような構成を用いることで、実施例1のメモリカードが奏する効果に加えて、たとえば、メモリカード130からメモリカード132へのデータの移動を、上述したようなセッションキー発生回路1502を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

〔実施例3〕

図12は、本発明の実施例3のメモリカード140の構成を説明するための概略ブロック図であり、実施例1の図5と対比される図である。

実施例1のメモリカード110の構成と異なる点は、メモリカード140内にコントローラ1420とデータの授受が可能なレジスタ1500が設けられていることである。

その他の構成は、図5に示した実施例1のメモリカード5の構成と同様であるので同一部分には同一符号を付して、その説明は繰り返さない。

図13は、図12で説明したメモリカード140を用いた配信モードを説明するためのフローチャートである。

図13においても、ユーザ1が、メモリカード140を用いることで、コンテンツサーバ10からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機100から、ユーザのタッチキー1108の操作等によって、コンテンツサーバ10に対して配信リクエストがなされる（ステップS100）。

コンテンツサーバ10においては、この配信リクエストに応じて、セッションキー発生部314が、セッションキー K_s を生成する（ステップS103）。

続いて、コンテンツサーバ10内の暗号化処理部316が、公開暗号化キー K_{Pmedia} により、セッションキー K_s を暗号化処理して、データバスBS1に与える（ステップS104）。

通信装置350は、暗号化処理部316からの暗号化コンテンツデータ $[K_s]K_{media}$ を、通信網を通じて、携帯電話機100のメモリカード140に対して送信する（ステップS106）。

メモリカード140においては、メモリインタフェース1200を介して、デ

ータバスBS3に与えられた受信データを、復号処理部1404が、秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する（ステップS108）。

5 続いて、配信モードにおいては、切換えスイッチ1408は、接点Paが閉じる状態が選択されているので、暗号化処理部1406は、接点Paから与えられる公開暗号化鍵KPCard(1)（ユーザ1のメモリカードにおける公開暗号化鍵）を、セッションキーKsにより暗号化して、データバスBS3に与える。

10 携帯電話機100は、暗号化処理部1406により暗号化されたデータ[KPCard(1)]Ksをコンテンツサーバ10に対して出力する（ステップS112）。

コンテンツサーバ10では、通信装置350により受信され、データバスBS1に与えられたデータ[KPCard(1)]Ksを復号処理部318が、セッションキーKsにより復号化処理して、公開暗号化キーKPCard(1)を復号抽出する（ステップS114）。

15 続いて、配信制御部312は、ライセンスキーKcを配信情報データベース304より取得し（ステップS116）、かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等のデータを生成する（ステップS118）。

20 暗号化処理部320は、配信制御部312からのライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等のデータを受取って、復号処理部318より与えられた公開暗号化キーKPCard(1)により暗号化処理する（ステップS120）。

25 暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキーKsにより暗号化して、データバスBS1に与える（ステップS122）。

通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc, License-ID, User-ID]KCard(1)]Ksをカード140に対して送信する。

メモリカード140においては、復号処理部1410がセッションキーKsに

より、復号処理を行ない、データ [Kc, License-ID, User-ID] Kcard (1) を抽出し (ステップ S126)、メモリ 1412 に格納する (ステップ S128)。

さらに、メモリカード 140 においては、復号処理部 1416 が、メモリ 1412 に格納されたデータ [Kc, License-ID, User-ID] Kcard (1) を復号し、復号されたデータ License-ID, User-ID をコントローラ 1420 が、レジスタ 1500 に格納する (ステップ 129)。

一方、サーバ 30 は、暗号化コンテンツデータ [Dc] Kc を配信情報データベース 304 より取得して、通信装置 350 を介して、メモリカード 140 に送信する (ステップ S130)。

メモリカード 140 においては、受信した暗号化コンテンツデータ [Dc] Kc をそのままメモリ 1412 に格納する (ステップ S132)。

以上のような動作により、メモリカード 140 は、音楽情報を再生可能な状態となる。

図 14 は、携帯電話機 100 内において、メモリカード 140 に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図 14 を参照して、携帯電話機のタッチキー 1108 等からのユーザ 1 の指示により、再生リクエストがメモリカード 140 に対して出力される (ステップ S200)。

メモリカード 140 では、コントローラ 1420 がレジスタ 1500 からライセンス ID データ License-ID、ユーザ ID データ User-ID 等を読み出す (ステップ S205)。

コントローラ 1420 は、ライセンス ID データ License-ID 等に含まれる情報に基づいて、復号可能なデータに対するリクエストであるかを判断し (ステップ S206)、復号可能と判断した場合は、携帯電話機のコントローラ 1106 に対して、再生許可通知を送信する (ステップ S208)。

携帯電話機 100 においては、セッションキー発生回路 1502 がセッションキー Ks を生成し (ステップ S210)、暗号化処理部 1504 が、公開暗号化

キー K_{Pmedia} によりセッションキー K_s を暗号化して（ステップS212）、データベースBS2に暗号化セッションキー $[K_s] K_{media}$ が出力される（ステップS214）。

5 メモリカード140は、データベースBS2を介して、携帯電話機により生成された暗号化セッションキー $[K_s] K_{media}$ を受け取り、公開暗号化キー K_{media} により復号し、セッションキー K_s を抽出する（ステップS216）。

10 続いて、メモリカード140は、メモリ1412から、暗号化されているデータ $[K_c, License-ID, User-ID] K_{card}(1)$ を読み出し、復号処理部1416が復号してライセンスキー K_c を抽出する（ステップS218）。

続いて、抽出したセッションキー K_s により、ライセンスキー K_c を暗号化し（ステップS219）、暗号化ライセンスキー $[K_c] K_s$ をデータベースBS2に与える（ステップS220）。

15 携帯電話機100の復号処理部1506は、セッションキー K_s により復号化処理を行なうことにより、ライセンスキー K_c を取得する（ステップS222）。

続いて、メモリカード140は、暗号化コンテンツデータ $[D_c] K_c$ をメモリ1412から読み出し、データベースBS2に与える（ステップS224）。

20 携帯電話機の音楽再生部1508は、暗号化コンテンツデータ $[D_c] K_c$ を、抽出されたライセンスキー K_c により復号処理し（ステップS226）、コンテンツデータを再生して混合部1510に与える（ステップS228）。

一方、ステップS206において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード140は、携帯電話機100に対して、再生不許可通知を送信する（ステップS230）。

ステップS230の状態では、メモリカード140は、状態SBにある。

25 図15は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

まず、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。また、携帯電話機102にも、メモリカード140と同様の構成を有するメモリカード142が装着されているものとする。

携帯電話機100は、まず、自身の側のメモ리카ード140と、受信側の携帯電話機102に挿入されたメモ리카ード142に対して、移動リクエストを出力する(ステップS300)。

さらに、携帯電話機100においては、セッションキー発生回路1502は、セッションキーKsを生成し(ステップS303)、公開暗号化キーK_{Pmedia}(a)を用いて、暗号化処理部1504がセッションキーKsを暗号化して(ステップS304)、データバスBS2を介して、メモ리카ード140に伝達し、さらに、たとえば、トランシーバモードではアンテナ1102を介して、暗号化されたセッションキーKsをメモ리카ード142に伝達する(ステップS306)。

メモ리카ード140においては、秘密復号キーK_{media}によりセッションキーKsを復号抽出する(ステップS318)。

同様にして、メモ리카ード142においても、秘密復号キーK_{media}により、セッションキーKsを復号抽出し(ステップS320)、さらに、セッションキーKsによりカード142の公開暗号化キーK_{Pcard}(2)を暗号化して(ステップS322)、メモ리카ード140に対して、暗号化されたデータ[K_{Pcard}(2)]Ksを送信する(ステップS324)。

メモ리카ード140においては、メモ리카ード142から送信された暗号化データをセッションキーKsにより復号化して、メモ리카ード142の公開暗号化キーK_{Pcard}(2)を復号抽出する(ステップS326)。

続いて、メモ리카ード140においては、メモリ1412からメモ리카ード140の公開暗号化キーK_{card}(1)により暗号化されているライセンスキーK_c、ライセンスIDデータLicense-IDおよびユーザIDデータUser-IDが読出される(ステップS328)。

続いて、復号処理部1416が、秘密復号キーK_{card}(1)により、ライセンスキーK_c、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを復号処理する(ステップS330)。

コントローラ1420は、このようにして復号されたライセンスキーK_c、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDの値を、レジスタ1500内のデータ値と置換する(ステップS331)。

さらに、暗号化処理部1414は、復号処理部1410において抽出されたメモリカード142における公開暗号化キーK_{Pcard}(2)により、ライセンスキーK_c、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを暗号化する(ステップS332)。

- 5 暗号化処理部1414により暗号化されたデータは、切換えスイッチ1408(接点P_cが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[K_c, License-ID, User-ID] K_{card}(2)をセッションキーK_sにより暗号化する(ステップS334)。

- 10 続いて、メモリカード140は、携帯電話機100を介して、メモリカード142に対して、暗号化されたデータ[[K_c, License-ID, User-ID] K_{card}(2)] K_sを送信する(ステップS336)。

- メモリカード142においては、メモリカード140から送信されたデータを復号処理部1410により、セッションキーK_sに基づいて復号化処理して、メモリ1412に格納する(ステップS339)。さらに、メモリカード142においては、復号処理部1416が、秘密復号キーK_{card}(2)に基づいて、データ[K_c, License-ID, User-ID] K_{card}(2)を復号し、復号されたライセンスIDデータLicense-ID、ユーザIDデータUser-IDをレジスタに格納する(ステップS341)。
- 15

- 20 一方、メモリカード140は、さらに、レジスタ1500に格納されたライセンスIDデータLicense-IDおよびユーザIDデータUser-IDを消去する(ステップS343)。

続いて、メモリカード140は、暗号化コンテンツデータ[D_c] K_cをメモリから読出し、メモリカード142に対して送信する(ステップS344)。

- 25 メモリカード142は、受信した暗号化コンテンツデータをそのままメモリ1412に格納する(ステップS346)。

以上のような処理を行なうと、ステップS343において、ライセンスIDデータLicense-IDおよびユーザIDデータUser-IDがメモリカード140のレジスタ1500からは消去されているので、メモリカード140は

「状態S B」となる。

一方、メモリカード142においては、暗号化コンテンツデータ以外にも、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等のすべてのデータが移動されているので、メモリカード142は「状態S A」となっている。

図16は、図12に示したメモリカード140において、携帯電話機100から携帯電話機102へ、暗号化コンテンツデータの複製を行なう処理を説明するためのフローチャートである。

図16を参照して、携帯電話機100が、メモリカード140およびメモリカード142に対して複製リクエストを出力する（ステップS400）。

続いて、メモリカード140は、暗号化コンテンツデータ[Dc] Kcをメモリ1412から読出し、メモリカード142に対して送信する（ステップS402）。

メモリカード142においては、メモリカード140から送信された暗号化コンテンツデータを、そのままメモリ1412に記録する（ステップS404）。

以上のような動作を行なうと、メモリカード140には、暗号化されたコンテンツデータ、ライセンスキーKc、ユーザIDデータUser-ID、ライセンスIDデータLicense-ID等のすべてのデータが残されているため、メモリカード140は再生可能な状態、すなわち、「状態S A」にある。

一方、メモリカード142は、暗号化コンテンツデータのみを有しているため、そのままでは再生処理を行なうことができない。したがって、この時点ではメモリカード142は、「状態S B」にある。

メモリカード142が状態S Aとなるためには、改めてコンテンツサーバ10から、ライセンスキーKc、ライセンスIDデータLicense-IDやユーザIDデータUser-ID等を取得する必要がある。

以上のような構成とすることで、実施例1のメモリカード110と同様の効果を奏する上に、ライセンスIDデータLicense-ID等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいので、動作に必要な処理量を低減できる。

なお、以上の説明では、コンテンツサーバ10からの暗号化データを復号するための回路は、携帯電話機に着脱可能なメモリカード内に組み込まれる構成としたが、たとえば、携帯電話機内部に作り込まれる構成としてもよい。より一般には、情報サーバにアクセスする端末機器に着脱可能なメモリカード内に組み込まれる構成であってもよいし、当該端末機器にあらかじめ組み込まれる構成であってもよい。

[実施例3の変形例]

実施例3のメモリカード140の再生処理では、ライセンスIDデータLicense-IDにより復号処理が可能であるかを判断する構成であった。このライセンスIDデータLicense-IDとしては、曲目の特定情報のみならず、再生回数の制限情報を含む構成とし、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。特に、メモリカード140では、ライセンスIDデータLicense-IDをレジスタ1500に保持する構成としたので、以下に説明するように再生処理を行なうたびに、ライセンスIDデータLicense-IDの内容を更新することが容易である。

以下に、このようなメモリカード140の再生処理を説明する。

図17は、携帯電話機100内において、実施例3の変形例のメモリカード140に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図17を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモリカード140に対して出力される（ステップS200）。

メモリカード140では、コントローラ1420がレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読出す（ステップS205）。

コントローラ1420は、復号化されたライセンスIDデータLicense-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-ID中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累計数が、再生可能回数の上限値を超えているかいないかを判断し（ステップS2

06)、再生可能回数を超えていないと判断した場合は、携帯電話機のコントローラ1106に対して、再生許可通知を送信する(ステップS208)。

携帯電話機100においては、セッションキー発生回路1502がセッションキー K_s を生成し(ステップS210)、暗号化処理部1504が、秘密復号キー K_{Pmedia} によりセッションキー K_s を暗号化して(ステップS212)、データベースBS2に暗号化セッションキーデータ $[K_s] K_{media}$ が出力される(ステップS214)。

メモ리카ード140は、データベースBS2を介して、携帯電話機により生成された暗号化セッションキー $[K_s] K_{media}$ を受け取り、秘密復号キー K_{media} により復号し、セッションキー K_s を抽出する(ステップS216)。

さらに、メモ리카ード140は、再生処理が行われることに応じて、レジスタ1500中のライセンスIDデータ $License-ID$ のうち、再生処理の累計数に関するデータを更新する(ステップ217)。

続いて、メモ리카ード140は、メモリ1412から、暗号化されているデータ $[K_c, License-ID, User-ID] K_{card}(1)$ を読み出し、復号処理部1416が復号してライセンスキー K_c を抽出する(ステップS218)。

続いて、抽出したセッションキー K_s により、ライセンスキー K_c を暗号化し(ステップS219)、暗号化ライセンスキー $[K_c] K_s$ をデータベースBS2に与える(ステップS220)。

携帯電話機100の復号処理部1506は、セッションキー K_s により復号化処理を行なうことにより、ライセンスキー K_c を取得する(ステップS222)。

続いて、メモ리카ード140は、暗号化コンテンツデータ $[D_c] K_c$ をメモリ1412から読み出し、データベースBS2に与える(ステップS224)。

携帯電話機の音楽再生部1508は、暗号化コンテンツデータ $[D_c] K_c$ を、抽出されたライセンスキー K_c により復号処理し(ステップS226)、コンテンツデータを再生して混合部1510に与える(ステップS228)。

一方、ステップS206において、コントローラ1420が復号処理は不可能であると判断した場合、メモ리카ード140は、携帯電話機100に対して、再

生不許可通知を送信する（ステップS230）。

以上のような構成とすることで、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

移動時には、再生情報内の再生回数を制限するライセンスIDデータLicensee-IDについて、メモリ1412に記録されたライセンスIDデータLicensee-IDを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンスIDデータLicensee-IDに変更して、新たな再生情報を構成する。このようにして、メモ리카ード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

〔実施例4〕

図18は、本発明の実施例4のメモ리카ード150の構成を説明するための概略ブロック図であり、実施例2の図10と対比される図である。

実施例2のメモ리카ード130の構成と異なる点は、メモ리카ード150内にコントローラ1420とデータの授受が可能なレジスタ1500が設けられていることである。

その他の構成は、図10に示した実施例2のメモ리카ード130の構成と同様であるので同一部分には同一符号を付して、その説明は繰り返さない。

図19は、メモ리카ード150の移動モードを説明するためのフローチャートであり、実施例2の図11と対比される図である。

図19を参照して、まず、図19においても、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。また、携帯電話機102にも、メモ리카ード150と同様の構成を有するメモ리카ード152が装着されているものとする。

携帯電話機100は、まず、自身の側のメモ리카ード150と、受信側の携帯電話機102に挿入されたメモ리카ード152に対して、移動リクエストを出力する（ステップS300）。

さらに、携帯電話機100においては、メモ리카ード150内のセッションキー発生回路1432は、セッションキーKsを生成し（ステップS312）、公

公開暗号化キー K_{Pmedia} を用いて、暗号化処理部 1430 がセッションキー K_s を暗号化して (ステップ S314)、たとえば、トランシーバモードではアンテナ 1102 を介して、暗号化されたセッションキー K_s をカード 152 に伝達する (ステップ S316)。

5 メモリカード 152 においても、復号処理部 1404 が、秘密復号キー K_{media} により、セッションキー K_s を復号抽出し (ステップ S320)、さらに、セッションキー K_s によりメモリカード 152 の公開暗号化キー K_{Pcard} (2) を暗号化して (ステップ S322)、メモリカード 150 に対して、暗号化されたデータ $[K_{Pcard}(2)] K_s$ を送信する (ステップ S324)。

10 メモリカード 150 においては、メモリカード 152 から送信された暗号化データをセッションキー K_s により復号化して、メモリカード 152 の公開暗号化キー $K_{Pcard}(2)$ を復号抽出する (ステップ S326)。

続いて、メモリカード 150 においては、メモリ 1412 からメモリカード 150 の公開暗号化キー $K_{card}(1)$ により暗号化されているライセンスキー K_c 、ライセンス ID データ $License-ID$ およびユーザ ID データ $User-ID$ が読出される (ステップ S328)。

続いて、復号処理部 1416 が、秘密復号キー $K_{card}(1)$ により、ライセンスキー K_c 、ライセンス ID データ $License-ID$ 、ユーザ ID データ $User-ID$ とを復号処理する (ステップ S330)。

20 コントローラ 1420 は、このようにして復号されたライセンスキー K_c 、ライセンス ID データ $License-ID$ 、ユーザ ID データ $User-ID$ の値を、レジスタ 1500 内のデータ値と置換する (ステップ S331)。

さらに、暗号化処理部 1414 は、復号処理部 1410 において抽出されたメモリカード 152 における公開暗号化キー $K_{Pcard}(2)$ により、ライセンスキー K_c 、ライセンス ID データ $License-ID$ 、ユーザ ID データ $User-ID$ とを暗号化する (ステップ S332)。

暗号化処理部 1414 により暗号化されたデータは、切換えスイッチ 1408 (接点 P_c が閉じている) を介して、さらに、暗号化処理部 1406 に与えられ、暗号化処理部 1406 は、データ $[K_c, License-ID, User-ID]$

D] Kcard (2) をセッションキーKsにより暗号化する(ステップS334)。

5 続いて、メモリカード150は、携帯電話機100を介して、メモリカード152に対して、暗号化されたデータ[[Kc, License-ID, User-ID] Kcard (2)] Ksを送信する(ステップS336)。

メモリカード152においては、メモリカード150から送信されたデータを復号処理部1410により、セッションキーKsに基づいて復号化処理して、メモリ1412に格納する(ステップS339)。さらに、メモリカード152は、
10 秘密復号キーKcard (2)に基づいて、データ[Kc, License-ID, User-ID] Kcard (2)を復号し、復号されたライセンスIDデータLicense-ID、ユーザIDデータUser-IDをレジスタ1500に格納する(ステップS341)。

一方、メモリカード150は、さらに、レジスタ1500に格納されたライセンスIDデータLicense-IDおよびユーザIDデータUser-IDを消
15 去する(ステップS343)。

続いて、メモリカード150は、暗号化コンテンツデータ[Dc] Kcをメモリから読出し、メモリカード152に対して送信する(ステップS344)。

メモリカード152は、秘密復号キーをそのままメモリ1412に格納する(ステップS346)。

20 以上のような処理を行なうと、ステップS342において、ライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等がメモリカード150からは消去されているので、メモリカード150は「状態SB」となる。

一方、メモリカード152においては、暗号化されたコンテンツデータ以外にも、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザ
25 IDデータUser-ID等のすべてのデータが移動されているので、メモリカード152は「状態SA」となっている。

以上のような構成を用いることで、実施例2のメモリカード130が奏する効果に加えて、たとえば、メモリカード150からメモリカード152へのデータ

の移動を、上述したようなセッションキー発生回路1502を有する携帯電話機を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

しかも、ライセンスIDデータLicense-ID等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいので、動作に必要な処理量を低減できる。

さらに、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。

[実施例5]

図20は、本発明の実施例5のメモリカード160の構成を説明するための概略ブロック図であり、実施例3の図12と対比される図である。

以下では、携帯電話機100に装着されるメモリカード160の公開暗号化キーK_{Pmedia}と、携帯電話機102に装着されるメモリカード162の公開暗号化キーK_{Pmedia}とを区別して、それぞれ、メモリカード160に対するものを公開暗号化キーK_{Pmedia}(1)と、メモリカード162に対するものを公開暗号化キーK_{Pmedia}(2)と称することにする。

また、これに対応して、公開暗号化キーK_{Pmedia}(1)で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キーK_{media}(1)と称し、公開暗号化キーK_{Pmedia}(2)で暗号化されたデータを復号可能であって、これとは非対称な秘密復号キーを秘密復号キーK_{media}(2)と称することにする。

このように、媒体固有の公開暗号化キーを区別することにより、以下の説明で明らかとなるように、メモリカードに複数の種類が存在する場合や、より一般的に、メモリカード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。

図20を参照して、本発明の実施例5のメモリカード160の構成が、実施例3のメモリカード140の構成と異なる点は、メモリカード160内にメモリカードという媒体に対応する公開暗号化キーK_{Pmedia}(1)の値を保持し、データバスBS3に公開暗号化キーK_{Pmedia}(1)を出力するためのKP

media 保持部 1440 が設けられていることである。

その他の構成は、図 12 に示した実施例 3 のメモリカード 140 の構成と同様であるので同一部分には同一符号を付して、その説明は繰り返さない。

図 21 は、図 20 で説明したメモリカード 160 を用いた配信モードを説明するためのフローチャートである。

図 21 においても、ユーザ 1 が、メモリカード 160 を用いることで、コンテンツサーバ 10 からの配信を受ける場合の動作を説明している。

まず、ユーザ 1 の携帯電話機 100 から、ユーザのタッチキーの操作等によって、配信リクエストがなされる（ステップ S100）。

メモリカード 160 においては、この配信リクエストに応じて、KPmedia 保持部 1440 から、公開暗号化キー KPmedia (1) をコンテンツサーバ 10 に対して送信する（ステップ S101）。

コンテンツサーバ 10 では、メモリカード 160 から転送された配信リクエストならびに公開暗号化キー KPmedia (1) を受信すると（ステップ S102）、セッションキー発生部 314 が、セッションキー Ks を生成する（ステップ S103）。

続いて、コンテンツサーバ 10 内の暗号化処理部 316 が、公開暗号化キー KPmedia (1) により、セッションキー Ks を暗号化処理して、データバス BS1 に与える（ステップ S104）。

通信装置 350 は、暗号化処理部 316 からの暗号化セッションキー [Ks] Kmedia (1) を、通信網を通じて、携帯電話機 100 のメモリカード 160 に対して送信する（ステップ S106）。

メモリカード 160 においては、メモリインタフェース 1200 を介して、データバス BS3 に与えられた受信データを、復号処理部 1404 が、秘密復号キー Kmedia (1) により復号処理することにより、セッションキー Ks を復号し抽出する（ステップ S108）。

以下の処理は、図 13 において説明した実施例 3 のメモリカード 140 の動作と同様であるのでその説明は、繰り返さない。

このような構成とすることで、メモリカード自身が、セッションキー Ks を送

る側（コンテンツサーバ10）に、公開暗号化キー $KPmedia(1)$ を送信した上で、配信を受けることができ、メモリカード160は、コンテンツデータを再生可能な状態となる。

5 図22は、携帯電話機100内において、メモリカード160に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図22を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストがメモリカード160に対して出力される（ステップS200）。

10 メモリカード160においては、この再生リクエストに応じて、 $KPmedia$ 保持部1440から、公開暗号化キー $KPmedia(1)$ を携帯電話機100に対して送信する（ステップS201）。

携帯電話機100では、メモリカード160からの公開暗号化キー $KPmedia(1)$ を受信して保持する（ステップS202）。

15 メモリカード160では、コントローラ1420がレジスタ1500からライセンスIDデータ $License-ID$ 、ユーザIDデータ $User-ID$ 等を読み出す（ステップS205）。

20 コントローラ1420は、ライセンスIDデータ $License-ID$ 等に含まれる情報に基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップS206）、復号可能と判断した場合は、携帯電話機のコントローラ1106に対して、再生許可通知を送信する（ステップS208）。

携帯電話機100においては、セッションキー発生回路1502がセッションキー Ks を生成し（ステップS210）、暗号化処理部1504が、公開暗号化キー $KPmedia(1)$ によりセッションキー Ks を暗号化して（ステップS212）、データバスBS2に暗号化セッションキー $[Ks]Kmedia(1)$ が出力される（ステップS214）。

メモリカード160は、データバスBS2を介して、携帯電話機により生成され、かつ暗号化されたセッションキー Ks を受け取り、秘密復号キー $Kmedia(1)$ により復号し、セッションキー Ks を抽出する（ステップS216）。

以下の処理は、図14において説明した実施例3のメモリカード140の動作と同様であるのでその説明は、繰り返さない。

このような構成とすることで、メモリカード自身が、セッションキー K_s を送る側（携帯電話機100）に、公開暗号化キー $KPmedia(1)$ を送信した上で、再生動作を行なうことが可能となる。

図23は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

まず、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。また、携帯電話機102にも、メモリカード160と同様の構成を有するメモリカード162が装着されているものとする。

携帯電話機100は、まず、自身の側のメモリカード160と、受信側の携帯電話機102に挿入されたメモリカード162に対して、移動リクエストを出力する（ステップS300）。

メモリカード160においては、公開暗号化キー $KPmedia(1)$ を携帯電話機100に対して送信し（ステップS301）、メモリカード162においては、公開暗号化キー $KPmedia(2)$ を携帯電話機100に対して送信する（ステップS301'）。

携帯電話機100は、公開暗号化キー $KPmedia(1)$ および公開暗号化キー $KPmedia(2)$ を受信する（ステップ302）。

さらに、携帯電話機100においては、セッションキー発生回路1502は、セッションキー K_s を生成し（ステップS303）、公開暗号化キー $KPmedia(1)$ および公開暗号化キー $KPmedia(2)$ を用いて、暗号化処理部1504がセッションキー K_s を暗号化する（ステップS304）。携帯電話機100は、データバスBS2を介して、メモリカード160に対しては暗号化セッションキー $[K_s] KPmedia(1)$ を伝達し、さらに、たとえば、トランシーバモードではアンテナ1102を介して、暗号化セッションキー $[K_s] KPmedia(2)$ をメモリカード162に伝達する（ステップS306）。

メモリカード160においては、秘密復号キー $Kmedia(1)$ によりセッションキー K_s を復号抽出する（ステップS318）。

同様にして、メモリカード162においても、秘密復号キー K_{media} (2)により、セッションキー K_s を復号抽出する(ステップS320)。

以下の処理は、図15において説明した実施例3のメモリカード140および142の動作と同様であるのでその説明は、繰り返さない。

5 このような構成とすることで、メモリカード自身が、セッションキー K_s を送る側(携帯電話機100)に、公開暗号化キー KP_{media} (1)および KP_{media} (2)を送信した上で、移動モードを行なうことが可能となる。

なお、複製モードについては、メモリカード160および162の動作は、実施例3のメモリカード140および142の動作と同様である。

10 また、以上の説明では、レジスタ1500が設けられているものとして説明したが、図5に示した実施例1のメモリカード110と同様に、レジスタ1500が設けられていない構成とすることも可能である。

15 なお、以上の説明では、コンテンツサーバ10からの暗号化データを復号するための回路は、携帯電話に着脱可能なメモリカード内に組み込まれる構成としたが、たとえば、携帯電話機内部に作りこまれる構成としてもよい。より一般には、情報サーバにアクセスする端末機器に着脱可能なメモリカード内に組み込まれる構成であってもよいし、当該端末機器にあらかじめ組み込まれる構成であってもよい。

20 さらに、図17において説明した実施例3の変形例のメモリカードの動作と同様に、ライセンスIDデータ $License-ID$ として、曲目の特定情報のみならず、再生回数の制限情報を含む構成とし、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。

[実施例6]

25 図24は、本発明の実施例6のメモリカード170の構成を説明するための概略ブロック図であり、実施例4の図18と対比される図である。

実施例4のメモリカード150の構成と異なる点は、第1の KP_{media} 保持部1440が、データバスBS3を介して他の媒体から送信された公開暗号化キー、たとえば、公開暗号化キー KP_{media} (2)を受信して保持し、暗号化処理部1430は、この公開暗号化キー KP_{media} (2)により、セッシ

セッションキー K_s を暗号化して、データベースBS3に与える構成となっていることである。

さらに、メモリカード170は、自身に対応した公開暗号化キー $KPmedia(1)$ を保持して、データベースBS3に出力することが可能な第2の $KPmedia$ 保持部1450を備える構成となっている。

その他の構成は、図18に示した実施例4のメモリカード150の構成と同様であるので同一部分には同一符号を付して、その説明は繰り返さない。

図25は、メモリカード170の移動処理を説明するためのフローチャートであり、実施例4の図19と対比される図である。

図25を参照して、まず、図25においても、携帯電話機100が送信側であり、携帯電話機102が受信側であるものとする。また、携帯電話機102にも、メモリカード170と同様の構成を有するメモリカード172が装着されているものとする。

携帯電話機100は、まず、自身の側のメモリカード170と、受信側の携帯電話機102に挿入されたメモリカード172に対して、移動リクエストを出力する(ステップS300)。

メモリカード172は、第2の $KPmedia$ 保持部1450から、自身に対応する公開暗号化キー $KPmedia(2)$ を携帯電話機102および100を介して、メモリカード170に送信し(ステップS301)、メモリカード170は、公開暗号化キー $KPmedia(2)$ を受信して、第1の $KPmedia$ 保持部1440に格納する(ステップS302)。

さらに、携帯電話機100の側においては、メモリカード170内のセッションキー発生回路1432は、セッションキー K_s を生成し(ステップS312)、公開暗号化キー $KPmedia(2)$ を用いて、暗号化処理部1430がセッションキー K_s を暗号化して(ステップS314)、たとえば、トランシーバモードではアンテナ1102を介して、暗号化セッションキー $[K_s]Kmedia(2)$ をメモリカード172に伝達する(ステップS316)。

メモリカード172においては、復号処理部1404が、秘密復号キー $Kmedia(2)$ により、セッションキー K_s を復号抽出する(ステップS320)。

以下の動作は、図19に示したメモリカード150および152の動作と同様であるのでその説明は繰り返さない。

以上のような構成を用いることで、メモリカード150の種類に応じて、公開暗号化キー K_{Pmedia} の値が異なるような場合等においても、実施例4のメモリカードが奏する効果と同様に、たとえば、メモリカード170からメモリカード172へのデータの移動を、上述したようなセッションキー発生回路を有する携帯電話機を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

しかも、ライセンスIDデータ $License-ID$ 等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、本実施例においても、ユーザがコンテンツデータを再生できる回数を制限する構成とすることも可能である。

なお、本実施例においても、図10に示した実施例2のメモリカード130と同様に、レジスタ1500を設けない構成とすることも可能である。

[実施例7]

実施例7のメモリカード180は、実施例4のメモリカード150の構成と異なって、配信サーバ、携帯電話機およびメモリカードの各々が、独自のセッションキーを生成する構成となっていることを1つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーを K_s とし、一方のメモリカード180の発生するセッションキーを K_{s1} とし、メモリカード180と同様の構成を有する他方のメモリカード182の発生するセッションキーを K_{s2} とする。

また、再生モードにおいて、携帯電話機側がメモリカードの生成するセッションキーを受け取るための公開暗号化キーを K_{Pp} とし、この公開暗号化キー K_{Pp} で暗号化されたデータを復号化できる秘密復号キーを K_p とする。

図26は、実施例7における携帯電話機101の構成を説明するための概略ブロック図である。